Public Health Information Technology
Functions and Specifications
(for Emergency Preparedness and Bioterrorism)
February 14, 2002

These Functions and Specifications will be updated regularly to represent completion of data specifications and architecture refinements. Updates can be found at:
www.cdc.gov/cic/functions-specs

Public health is practiced by an array of local, state and federal organizations that are further divided into functionally organized units around clinical, health department, laboratory, disease program and other operational divisions. The complex responsibilities and interactions between these public health partners necessitate significant coordination of information technology and information sharing methodologies to meet bioterrorism and public health preparedness objectives. This document contains partner and CDC functions, industry standards and detailed specifications necessary to have a secure, coordinated public health IT system capable of acquiring, managing, analyzing and disseminating public health information to meet these challenges. The specifications included herein are based on industry data and systems standards, most of which have been identified in related national initiatives like the National Electronic Disease Surveillance System (NEDSS) and the Health Alert Network (HAN). As such, these standards and specifications represent a part of a broader public health systems and data architecture.

This document identifies bioterrorism and public health preparedness functions and describes how these functions should be implemented using identified standards and standards-based specifications to build a coordinated system. The system will enable the secure, immediate exchange of critical health data (surveillance, possible cases, contacts, lab, clinical, personnel, etc.) between clinical partners, public health agencies and labs and, as appropriate, federal agencies. It will support the appropriate management and presentation of information to public health decision makers at a variety of levels. To achieve the sharing of software and systems and to be able to reliably exchange data, adherence to specific data and systems specifications (which in turn adhere to appropriate national standards), is required and will be evaluated.

Each IT function may be referenced in several places in cooperative agreement guidance. A reference to a specific function requires full compliance with the stated functions, standards and specifications. The IT function describes general functional capabilities specifications for how those capabilities need to be accomplished to work as a cohesive whole and the standards on which these specifications are based. The functions also identify who has responsibility for its fulfillment, the methods through which fulfillment will be evaluated, and, in some cases, additional, not yet completed data specifications that will be finalized in the coming months.

Specifications are Included for the Following IT Functions:

1. **The Automated Exchange of Data Between Public Health Partners -** To securely and automatically exchange information, as appropriate, between two computer systems to achieve a “live” network for data exchange between partners in public health

2. **The Use of Electronic Clinical Data for Event Detection -** To receive, manage and process electronic data from care systems at clinical care sites, laboratories, or their proxies

3. **Manual Data Entry for Event Detection and Management -** To accumulate, manage and process information manually entered via a web browser at a health agency or remote site

4. **Specimen and Lab Result Information Management and Exchange -** For laboratories involved in public health testing, to receive laboratory requests, accept specimen and sample data, manage these data and immediately report electronic results to public health partners

5. **Management of Possible Case, Contacts and Threat Data -** To electronically manage, link and process the different types of data (possible cases from detection, possible contacts, facility, lab results, prophylaxis and/or vaccination, adverse events monitoring and follow-up)

6. **Analysis and Visualization -** To analyze, display, report and map accumulated data and share data and technologies for analysis and visualization with other public health partners

7. **Directories of Public Health and Clinical Personnel -** To participate in and maintain directories of public health participants (including primary clinical personnel), including participant roles and contact information

8. **Public Health Information Dissemination and Alerting -** To receive, manage and disseminate alerts, protocols, procedures and other information for public health workers, primary care providers, and public health partners in emergency response

9. **IT Security and Critical Infrastructure Protection -** To ensure that sensitive or critical electronic information and systems are not lost, destroyed, misappropriated or corrupted

Additional Content:

- List of Data Specifications to be completed in early 2002
- CDC commitments to support these functions

Public Health Information Technology
Functions and Specifications
(for Emergency Preparedness and Bioterrorism)
February 8, 2002

Function #1 – The Automated Exchange of Data Between Public Health Partners

This function involves the ability to securely and automatically send and receive information, as appropriate, between two computer systems, to achieve a “live” network for data exchange between partners in public health. Specific data and technical standards for event detection, the management of possible cases, case contacts, potential threats, specimens, lab results, alerts and procedures are referenced in other parts of this appendix. The specifications for this function define the technical infrastructure necessary to exchange this information between a computer system at one public health partner and a computer system at another public health partner.

This function should be implemented for the purpose of sending and receiving information between partners in public health including state and local public health agencies that run information systems. It should be used by laboratories participating in emergency preparedness and response activites and, at least in a sending mode, by participating clinical sites. The presentation of information to clinical sites and other participants in public health may be accomplished by public and secure web-based viewing via technologies identified in other included functions.

Technical Specifications

One side of each system-to-system data exchange will install and maintain an ebXML compliant SOAP web service that can be reached via an HTTPS connection after appropriate authentication. The other side of the system-to-system data communication can be behind a firewall where a traditional HTTPS port is open (as is normal for secure web access). Bi-directional messaging is possible through this implementation, but some partner to partner exchanges will have authenticated web services on both sides of the “conversation.” Messages will be in the industry standard ebXML format and will include standardized HL7 Version 2.3, HL7 Version 3.0, X12 and LDIF message content. Software to enable public health ebXML messaging will be available for download from the CDC.

Sensitive data should be encrypted prior to being sent through the secure HTTPS data transport. Stored data from messages should be protected using strong authentication and other security precautions identified in Function #9 (IT Security and Critical Infrastructure Protection). Message creation and parsing to support system-to-system data exchange can be accomplished via a dedicated interface engine, HL7 message and translation software components, or integration broker technologies running on Windows NT / 2000, LINUX or UNIX servers. The ability to translate and manipulate LOINC, SNOMED, ICD and CPT codes and to map local codes into these standards will be necessary to process some messages. Specific messages, including their message structures and vocabularies, are referenced in other functions and/or identified for further specification at the end of this document.

Systems participating in this function need to be connected to the Internet at all times (they should not require manual dial-up each time for connection). The connection shall be a minimum of 56Kbps with a strong recommendation for 384 Kbps or greater.

Evaluation of Function

Regular testing of this function with reporting on completed data exchange between relevant public health partners should be initiated by the end of 2002. Successful fulfillment of this function will mean, for example, that a message can be sent from the CDC to appropriate public health agencies (state and/or local) covering every jurisdiction in the United States and its associated territories or that an electronic message about a bioterrorism pathogen could originate in a clinical or lab setting, be immediately sent via secure means, and no necessary human intervention, to the responsible local or state health department, where it would be immediately available for processing and analysis. The message would also be immediately electronically sent in linked, but de-identified form to the appropriate federal agencies.

Function #2 – The Use of Electronic Clinical Data for Event Detection

This function involves the receipt, management and processing of electronic data from clinical care sites, laboratories or their proxies, for the purpose of surveillance for the identification of a possible bioterrorism or other public health events. The data may originate in clinical care, laboratory information management or admission discharge and transfer systems and may be provided directly from clinical care sites or through their proxies. Accumulated data need to be stored in the specified standard data format, to be analyzable by humans and automated detection algorithms, to be presentable in tabular, geospatial and other report formats, and to be automatically sent, in appropriate aggregate or individual form, to other public health participants.

This function should be implemented by state and/or local public health agencies receiving electronic data from clinical sites and their surrogates. If implemented by the local health department, specified[1] data will be sent in real time to the responsible state health department, and in turn, other specified[2] data will be sent to federal agencies. If implemented by a state health department for a particular jurisdiction, local public health officials should be provided secure access to the data for their jurisdiction.

Technical Specifications

Data will be received by public health partners via ebXML messaging identified in Function #1 (The Automated Exchange of Data Between Public Health Partners). Data storage should occur using the NEDSS logical data model specification of the HL7 Reference Information Model and extensions made to accommodate syndromic and other clinical data that will be completed in early 2002[3]. Data accumulated for this purpose need to be stored in a format compatible with the NEDSS / HL7-compatible Logical Data Model so that general analytic and reporting tools can be developed. The data repository should be able to associate incoming data with appropriate existing data (e.g., a report of a disease in a person who had another condition previously reported), and should function so that data can be accessed by standards-based interaction with commercial products for reporting, statistical analysis, geographic mapping and automated outbreak detection algorithms, as well as the processing of queued data from and for electronic messages. The data repository should implement common database technology (e.g., Sybase, Oracle or SQL Server) running on servers using Windows NT / 2000 /XP, LINUX or UNIX and supporting ODBC, ANSI standard SQL and JDBC access.

Evaluation of Function

Regular evaluation of the number of hospital and primary care sites that are functioning (as evidenced by receiving data from each site) compared with the total number of possible hospital and primary care sites in a state should be accumulated by the end of 2002.

Function #3 Manual Data Entry for Event Detection and Management

This function involves the capability to accumulate, at a public health agency, manually entered syndromic and other data (utilization, clinical census, aggregate diagnoses) from clinical points of care that may provide surveillance for the identification of a possible bioterrorism or chemical attack. It should also support heightened surveillance capabilities (more sensitive and detailed) for implementation during high profile events or after the identification of a likely case. Accumulated data need to be stored in the specified standard data format, so they may be analyzable by humans and automated detection algorithms, to be presentable in tabular, geospatial and other report formats, and to be automatically sent, in appropriate aggregate or individual form to other public health participants as specified in Function #1 (The Automated Exchange of Data Between Public Health Partners) and in the relevant message format. Systems to detect possible events need to link seamlessly (including the ability to track back to specific cases) with systems for case management, contact tracing and other public health follow-up and response activites.

This function should be implemented by state and/or local public health agencies performing electronic surveillance. If implemented by the local health department, specified[1] data will be sent in real time to the responsible state health department and, in turn, specified[2] data will be sent to appropriate federal agencies. If implemented by a state health department, local public health officials will be provided secure access to their jurisdictional data.

Technical Specifications

The storage of data accumulated in this manner should follow the data specifications identified in Function #2 (The Use of Electronic Clinical Data for Event Detection) including the NEDSS logical data model specification of the HL7 Reference Information model and extensions identified in early 2002[3]. Secure browser-based data entry should be used for data input and results reporting from and to primary care clinical care sites and other sources (e.g., infection control practitioners, small laboratories). Web browser-based data systems should be developed using commercial application server technology as part of a multi-tiered web development system using open-platform web servers (e.g., Apache, Microsoft's IIS, Netscape) running on Windows NT / 2000 /XP, LINUX or UNIX and supporting generic web browsers (HTML 3.0+ / Java). The web server, the application server and the database server should be separate tiers of this system. JavaScript for field-based data validation in the browser and EJB, CORBA, or DNA (DCOM) components on the server can be implemented for application logic. Application servers, regardless of physical platform, should be able to run shared JAVA code. Data delivery to an associated database should use ANSI standard SQL and ODBC or JDBC connectivity. Security over the Internet should be implemented using strong authentication, (Secure Sockets Layer (SSL) capable server and industry standard client certificates or token-based for authentication and selective authorizations). Firewalls will be necessary to protect accumulated data as described in Function #9 (IT Security and Critical Infrastructure Protection).

Evaluation of Function

Regular evaluations of the number of hospital, local health department and other primary care sites that are functioning (as evidenced by receiving data from each site) compared with the total number of possible hospital and primary care sites should be accumulated by the end of 2002.

Function #4 – Specimen and Lab Result Information Management and Exchange

This function involves the ability to receive laboratory requests, accept specimen and sample data, manage these data and immediately report electronic results to public health partners. The function draws on the same infrastructure as Function #1 (The Automated Exchange of Data Between Public Health Partners). It also involves specific capabilities to receive specimen information and lab result reports from labs without electronic laboratory reporting and to manage and process data internal to the lab in Laboratory Information Management Systems (LIMS) in such a way that electronic lab result reports will be immediately available.

This function should be used by public health laboratories and public health partner laboratories with electronic information systems. Specimen and sample data need to be accumulated by other public health partners using the same data and data exchange standards as public health laboratories. Accumulated data need to be automatically sent, in appropriate aggregate or individual form to other public health participants as per Function #1 (The Automated Exchange of Data Between Public Health Partners).

Technical Specifications

Data associated with these activites need to be stored in HL7 compatible data formats. Coding of request and results messages with the LOINC and SNOMED vocabularies is a necessary component of the reliable interchange of data. Information exchange and message creation and parsing should be fulfilled as per Function #1 (The Automated Exchange of Data Between Public Health Partners). Web systems for receiving specimen information and for the entry of small numbers of lab results by facilities that are unable to exchange messages may also be supported. Web based results reporting should only be supported for entry to an organization participating in Function #1. Web based results entry does not fully meet the requirements for a “live” network for data exchange between partners in public health.

Evaluation of Function

Regular evaluation of the number of public health laboratories that can electronically manage specimen and results data, can code data with the appropriate vocabularies, and can automatically exchange data with partner public health organizations should initiated by the end of 2002.

Function #5 – Management of Possible Case, Contacts and Threat Data

This function involves having public health bioterrorism and preparedness systems that can manage all relevant data types and trace possible cases from detection, through lab testing and confirmation, possible prophylaxis and/or vaccination, adverse events monitoring, follow-up and possible death. These needs put a high emphasis on maintaining associated demographic (home and occupation), contact (communicable disease tracing), clinical, geospatial and event data (threat, facility, etc.) in forms that can be readily associated, re-linked and processed. Registry de-duplication and automated record linking capabilities should be established to ease data exchange between partners. Emphasis should be given to the development of management systems that allow for the management of public health surveillance and response data beyond the needs of case detection and alerting.

This function should be implemented by either a state and/or local health department for every jurisdiction in the United States and its associated territories.

Technical Specifications

The input and management of possible case and contact data should comply with the standards and specifications in Functions #1-4 above. Potential cases should be “linked” and traceable from detection via electronic sources of clinical data or manual entry of potential case data through confirmation via laboratory result reporting. Data storage should be implemented as specified in Function #2 (The Use of Electronic Clinical Data for Event Detection) using the NEDSS logical data model specification of the HL7 Reference Information Model and extensions thereof (completed for this purpose in early 2002). Data input and management should be implemented via Web browser-based systems as identified in Function #3 (Manual Data Entry for

Event Detection and Management). Lab results should be derived from systems as identified in Function # 4 (Specimen and Lab Result Information Management and Exchange) and exchanged as per Function #1 (The Automated Exchange of Data Between Public Health Partners).

Evaluation of Function

Local and state public health agencies should initiate the evaluation of this function including consideration of tracking threats and cases and managing case contacts. A program of annual validation should be managed by the local and state public health agencies.

Function #6 – Analysis and Visualization

This function involves the ability to analyze, display, report and map data accumulated and stored according to the specifications in Functions #1 through 5 above. Selective data reporting according to user need-to-know, statistical analysis, Geographic Information Systems (GIS) and other visualization, display and mapping functions will be implemented using COTS (commercial off the shelf software) solutions through industry standards for access to the data repository. This function also involves the ability to install and operate outbreak detection algorithms that operate via standards base access to the specified data structures.

This function should be implemented by state and/or local health departments, which are supporting the storage and management of data as per Functions #2-5.

Evaluation of Function

Public health agencies that support information systems should evaluate their ability to clearly present, analyze and report accumulated data to meet detection, management and preparedness programmatic needs. Formal usability analysis should be considered for all systems and custom built reports.

Technical Specifications

Commercial reporting systems (e.g., Crystal Reports or Actuate), statistical analyses software (e.g. SAS or SPSS) and GIS software (e.g., ArcView or MapInfo) will be integrated using ODBC and JDBC data access. Security and access control will be applied for remote access over public networks using SSL and certificate or token-based authentication with appropriate authentication and authorization.

Function #7 – Directories of Public Health and Clinical Personnel

This function involves the support of a directory of public health participants (including primary clinical personnel) and participants' roles and contact information for every jurisdiction. These directories will be in a form as to be immediately usable for the direct or relayed transmission of public health notifications (via e-mail, pagers, voicemail, and/or automated faxing). The directories will also be regularly exported, in a specificed[4] data format, to appropriate public health partners (local, state and federal) to ensure redundant and complementary functions. These directories can also be used to support authentication of identified personnel to restricted access electronic resources. The directories should, minimally, be able to support the retrieval of individuals based on name, public health role, organizational affiliation and geographical location.

This function should be implemented by a state and/or local health department to achieve coverage of the United States and its associated territories.

Technical Specifications

These directories will present a Lightweight Directory Access Protocol (LDAP v3.0) standard-based service to allow data access and sharing across multiple computer systems and, as appropriate, organizational boundaries. Directory information transfer and sharing will be supported by a standard message format based on the LDAP Data Interchange Format (LDIF) standard. Data fields in the directory will use X.500 standards for field type and length. Implementation for individuals will be based on existing LDAP standards as embodied in the person, organizationalPerson, and inetOrgPerson LDAP object classes. Complete specification for LDIF format of LDAP data fields is in draft form and will be reviewed by public health partners and published in early 2002.[4] LDIF data messages should be exchanged between public health partners as content of ebXML messages as described in Function #1 (The Automated Exchange of Data Between Public Health Partners).

Evaluation of Function

Regular evaluation by local and state public health agencies of coverage (percent of target individuals included), effectiveness, and accuracy of the directories should be initiated by the end of 2002.

Function #8 – Public Health Information Dissemination and Alerting

This function includes the ability to receive, manage and disseminate alerts, protocols, procedures and other information for dissemination to public health workers, primary care physicians, public health laboratorians, and public health partners in emergency response. It includes the ability to “push” information via messages and allow participants to “pull” information via the browsing of secure web sites. It may also include the support of interactive communication sites for threaded discussion capabilities.

Message distribution between public health partners will be in a specified format[5]. Immediate distribution to public health partners should be possible through one or more mechanisms (e-mail, pagers, voicemail, and/or automated faxing). Based on specified[5] message descriptors for level of criticality and for involved program areas, the responsible organization will be able to:

- Immediately pass on highly critical information (as specified in message format) to personnel in their directory and, as needed recursively, to sub-jurisdictions with directories so that all public health and clinical personnel can be notified
- Edit messages for local needs and then transmit when they contain less time critical information

- Direct information to appropriate audiences based on the agreed to message subject descriptors and corresponding recipient descriptors in the public health directories identified in Function #8 (Directories of Public Health and Clinical Personnel)
- Securely archive information for subsequent viewing and facilitate secure discussion of public health issues through authenticated access to an appropriate web site

This function should be implemented, by a responsible local and/or state health department for full coverage of the United States and its associated territories. This function will serve critical and non-critical notification purposes among public health participants.

Technical Specifications

Message formats will be developed with content and descriptors in compatible XML format. Specific presentations of content will be translatable and shareable in ASCII text format for e-mail messages and faxes.

Web browser-based data systems should be developed using commercial application server technology as part of a multi-tiered web development system using open-platform web servers (e.g., Apache, Microsoft's IIS, Netscape) running on Windows NT / 2000 /XP, LINUX or UNIX and supporting generic web browsers (HTML 3.0+ / Java). Secure web presentation over the Internet should be implemented using strong authentication, (Secure Sockets Layer (SSL) capable server and industry standard client certificates or token-based for authentication and selective authorizations). Systems should be protected according to Function #9 (IT Security and Critical Infrastructure Protection).

Evaluation of Function

Regular evaluation by local and state public health agencies of coverage (the percent of individuals reached by messages and in what timeframe) should be initiated by the end of 2002. Periodic exercises should be employed to assess the effectiveness of the function.

Function #9 - IT Security and Critical Infrastructure Protection

This capability involves assuring that access to sensitive or critical information and information systems is not lost, destroyed, misappropriated or corrupted by a internal or external malefactor or by systems failure or catastrophic event and that information is protected is ways that meet or exceed HIPAA standards. The function should also assure that processes cannot be initiated or controlled by unauthorized individuals and that continuity of operations can be maintained subsequent to a catastrophic event.

This function should be implemented for all state and local health departments and other public health related organizations including clinical care and laboratory providers who run electronic information systems.

Technical Specifications

Client and server X.509 digital certificates or comparable strong authentication methodology should be required for access to sensitive or critical resources from the Internet. Role-based, mandatory access control protocols, as well as realistic and effective policies for use and administration of information technology resources, should be established. Security patches and configuration corrections should be applied promptly. Desktop and server based virus scanning, intrusion detection, network vulnerability analysis including port scanning, security policy monitoring, regular penetration testing and active threat intelligence should be employed. Continuity of operations planning and procedure implementation should incorporate man-made and natural catastrophic event management, routine offsite back-ups and hot site considerations.

Security policies will be implemented with authentication based on industry standard X.509 certificates, secure tokens, and other applicable means as identified; access and control of data via selective integrated repository authorization; an encryption engine and appropriate use of encrypted data; and access control through a firewall by data routing to programs and other organizations. Firewalls will need to securely provide access to an ebXML SOAP receiver to present a service for secure Internet receipt of public health information as well as secure access to restricted access web sites.

Evaluation of Function

External verification of security and continuity processes and technology for public health agencies that support critical information systems should occur on at least a yearly basis. Independent validation and verification should include disaster simulations and intrusion detection.

CDC Commitments to Support These Functions

CDC systems developed or promoted to support these activities will:

- Will integrate into existing state or local strong authentication and authorization technologies using a single approach.
- Will use a common methodology for the exchange of data between partner systems (ebXML, SOAP, HTTPS and for some, not sensitive data SMTP)
- Will require only one single directory of public health, clinical and participant personnel (LDAP directory) for any particular jurisdiction.
- Will support standards-based access to major database management systems
- Will use the same implementation environment wherever possible and will be sensitive to the multiple operating systems and database management systems that exist on servers at state and local levels
- Will use single data and vocabulary standards, wherever possible, to describe the same data elements

The CDC will implement a central directory capability to provide effective linkage between state and local level directories, a central search capability, and where appropriate, an integration of public health organizational data.

The CDC will provide consultation and technical assistance on all communication and information technology components as well as the implementation of IT Functions and Specifications

The CDC will promote these industry standards-based approaches, wherever possible to other groups and organizations.

List of Additional Specifications to be Detailed by Public Health Partners

While a great number of data specifications (based on national standards like HL7, SNOMED, LOINC, ISO codes) have already been specified for the NEDSS Logical Data Model and are being specified for the HL7 Version 3.0 compatible Public Health Notification Messages, more work needs to be done by the public health partners to agree on complementary data specifications in several areas related to Emergency Preparedness, Bioterrorism, Chemical Event Detection and Response. In early 2002, the CDC will initiate several focused data modeling sessions (for data specification) and joint application development sessions (for necessary procedures) for public health partners to solidify standards-based data specifications and workflows in several areas listed below.

[1] Public Health Notification messages including data fields and vocabulary for the exchange of possible cases, contacts and bioterrorism surveillance data between local and state health departments to be specified in early 2002.

[2] Public Health Notification messages including data fields and vocabulary for the exchange of linked, but de-identified, possible cases and bioterrorism surveillance data between state health departments and federal agencies to be specified in early 2002.

[3] HL7 compatible extensions to the NEDSS logical data model to accommodate clinical and syndromic data.

[4] An LDIF exchange format, based on X.500 naming standards, to exchange data between LDAP directories is in draft form. This draft will be reviewed and specified through a formal partner joint application development session in early 2002.

[5] Formal modeling in the HL7 process to specify data fields and vocabulary for describing message criticality (and derivative message processing procedures), message content type descriptors (subject areas, sender type, recipient type) and potentially interested parties, etc.